AMENDMENTS TO THE SPECIFICATION:

Please replace paragraph [03] beginning at page 2, with the following rewritten paragraph:

[03] Since the transaction is online, it is often more precise to refer to a user computer system, a merchant computer system and an issuer computer system. Thus, for a transaction to take place, the user computer system connects to the merchant computer system and interacts, then the user computer system and/or the merchant computer system connects to the issuer computer system and interacts, with the merchant computer system typically interacting with the issuer computer system, if at all, through an acquirer computer system that in turn interacts with the issuer computer system via a payment network, such as the ~~VisaNet(TM)~~ VISANET(TM) network operated by Visa International. In card systems, "issuer" is the term typically used to refer to the entity that issues a card (or a card number) to a user for the purpose of making purchases upon presentation of the card or the card number. Typically the entity is a bank or other financial institution or an agent of a bank or financial institution. The term "acquirer" refers to the entity that accepts the transaction details from the merchant and effects a transfer of funds from the issuer to the acquirer on behalf of the merchant. In some cases, the issuer and acquirer might be the same entity. The systems might be large computer processing systems, personal computers, handheld devices, wireless devices, cellular telephones with data capability, or other computing devices.

Please replace paragraph [11] beginning at page 5, with the following rewritten paragraph:

[11] In this specific scheme, the OTN 10 is a 16-digit number, like other credit and debit card numbers, and is divided into fields as shown in Fig. 1. As shown, the first field 12 is one digit indicative of the payment system used by the issuer with that user. By way of example, "3" indicates ~~American Express~~one payment system, "4" indicates ~~Visa International~~another payment system, "5" indicates ~~MasterCard~~yet another, "6" indicates

~~Discover~~yet another, etc. The second field 14 is four to six digits that are associated with the particular issuer. The third field 16 is four digits that are associated with the particular user. The first three fields (9 to 11 digits) do not change from transaction to transaction. The last digit 20 is a checksum value dependent on the first fifteen digits, so there are only four to six digits that can change independently from transaction to transaction. Those four to six digits are referred to as a "Message Authentication Code" or "MAC" 18. The MAC can be a cryptographic hash of transaction parameters, such as those mentioned above.

A2 cont

Please replace paragraph [13] beginning at page 5, with the following rewritten paragraph:

A3

[13] A more general description of such an online transaction is shown in the swim diagram of Fig. 2, which illustrates interactions between a user system, a merchant system and an issuer system. The steps of the swim diagram are labeled "S1", "S2", "S3", etc. As shown there, the user interacts with the merchant to define parameters of the transaction, such as what products or services would be purchased, quantities, and the like (step S1). The user system generates a one-time number 22 from user and transaction data and sends that one-time number to the merchant system (S2). The merchant system then uses that number to request the authorization (S3) and to begin the payment process with the issuer. The one-time number encodes for the user identification, as well as being a function of transaction details. Once the issuer receives a request (S4) from the merchant, the issuer system can verify the validity of the OTN relative to the transaction details 24 used to generate that OTN (S5). Since the OTN encodes for the user ID, the issuer can determine which user is party to the transaction. If the one-time number encodes for a valid user ID and correctly encodes for the selected transaction details, and sufficient funds are available to the identified user, then the issuer responds to the merchant's authorization request with an approval (S6). The merchant then proceeds with the transaction and notifies the user as needed (S7).

Please replace paragraph [14] beginning at page 6, with the following rewritten paragraph:

[14] The above scheme does not scale well, as only 10,000 distinct customers of a given issuer can be supported since only four digits are usable for customer identification. The above scheme also has a problem in that the probability of fraud is not greatly reduced. Since only four to six digits are allocated for the MAC, a dishonest merchant or interloper can easily generate all the ten thousand to one million possible MACs and submit fraudulent transactions and some of them will be accepted. A merchant that processes one legitimate transaction can use the received OTN as a starting point to generate an unauthorized transaction and submit the transaction to an issuer. On average, if a merchant automatically generates a large number of such unauthorized transactions, as many as one per 10,000 unauthorized transactions will succeed.

Please replace paragraph [15] beginning at page 6, with the following rewritten paragraph:

[15] Other OTN card schemes provide more protection against fraud, such as the issuer-generated numbers used by some companies, such as Orbiscom. Fig. 3 is a swim diagram of such a scheme. With this scheme, the OTNs do not necessarily match fields with the user's permanent number, which allows for more variability in the MAC. As with the Microsoft scheme, each user system includes software provided to handle OTN generation. In the issuer-generated approach, however, the user authenticates with the issuer (S10, S11) and the issuer generates the OTN (S12). The OTN may encode for other capabilities, such as a transaction value or time limit, or for limitation to a specific merchant.

Please replace paragraph [16] beginning at page 6, with the following rewritten paragraph:

[16] Once the user system obtains the OTN (S13), the user sends the OTN to the merchant along with other transaction details (S14). The merchant processes the transaction in the normal way (S15) using the desired payment network and forwards the OTN and other details to the merchant's acquirer (i.e., sends a message to a payment network). The acquirer then sends the OTN and transaction amount to the issuer, directly or indirectly (S16). The issuer then associates the OTN with the appropriate customer and proceeds with the transaction (S17). After processing the request, the issuer either approves or declines the transaction and sends the response to the acquirer (S18). The acquirer forwards the response to the merchant and the merchant notifies the customer as to whether the transaction has been approved or declined (S19).

Please replace paragraph [36] beginning at page 9, with the following rewritten paragraph:

[36] Fig. 5 is a swim diagram illustrating a novel process for using one-time numbers for online transactions according to one embodiment of the present invention. A typical transaction begins when a user begins to interact with a merchant to select and provide details for a particular transaction. For example, the user may direct the user's browser to a merchant's web server and browse web pages thereon. Such merchant web pages might comprise an online catalogue with payment and check capability. To initiate the transaction (S50), the user generates a one-time number from user and transaction data (S51). As illustrated by the exemplary one-time number format shown in Fig. 6, the one-time number 60 might comprise a one-digit payment network ID 62, a four-digit bank (issuer) ID 64, a ten-digit transaction ID 66 and a one-digit checksum 68. The transaction ID can be a random number, a pseudorandom number or a determinant function of the user's permanent card number or other user ID and transaction details. The user sends a message to the issuer (S52) when the message includes a user ID or

other data that would allow the issuer system to associate the message with a particular user, the one-time number (or just the transaction ID) and transaction details as might be needed by the issuer to verify the validity of the transaction ID. The user system and the issuer system might optionally have previously performed an authentication process so that the user system can rely on the authenticity of the messages from the user system.

(Please replace paragraph [37] beginning at page 10, with the following rewritten paragraph:)

[37] As one of the online transaction interaction between the user system and the merchant system, user system will send (S53) the one-time number to the merchant and the merchant will process the transaction (S54). As part of processing the transaction, the merchant system submits (S55) a payment authorization request to the issuer system, most likely via a payment network that can determine the issuer associated with the transaction from the one-time number. For example, a merchant system might pass the one-time number to an acquirer system, which would determine an appropriate payment network from the payment ID of the one-time number and the appropriate payment network would determine the issuer involved in the transaction from the bank ID of the one-time number.

5 A Cont

(Please replace paragraph [38] beginning at page 10, with the following rewritten paragraph:)

[38] Since the issuer system had recorded the one-time number in association with a user ID in a previous step, when the issuer system receives a message containing the one-time number from the merchant system, the issuer system can match the one-time number with the user involved in the transaction (S56). The issuer system can then process the transaction (S57) in a conventional manner, such as by checking an available credit limit of the user associated with the transaction and executing optional fraud prevention procedures. The issuer system can then either approve or deny the transaction and

communicate its decision to the merchant system, typically via the payment network used. The merchant can then proceed with the transaction (S58) with the user given the response from the issuer system.

A5 Amt

Please replace paragraph [39] beginning at page 10, with the following rewritten paragraph:

[39] In a specific embodiment, one-time card numbers (OTNs) have the format shown in Fig. 6. As shown there, the OTN 60 comprises sixteen digits, where the sixteenth digit is a checksum. The first field 62, 64 is five digits that identify the payment network and issuer. The second field 66 is ten digits that vary from transaction to transaction, even for the same user. These ten digits are referred to herein as the "transaction identifier" or "transaction ID" 66. In other variations, the total number of digits might be more or less than sixteen, bases other than ten might be used, and the number of different issuers that are accommodated could be more or less than the five digits of the first field would accommodate.

Please replace paragraph [46] beginning at page 12, with the following rewritten paragraph:

A6

[46] Fig. 7 is a swim diagram illustrating such a process. As shown there, the client first generates the challenge, C (S70). The client signs C using the client's private key, PRIVK, to form the challenge signature, $S_{PRIVK}(C)$ (S71). The client then sends the server (S72) the client's ID, C and $S_{PRIVK}(C)$. The server uses the client's public key, PUBK, to verify that $S_{PRIVK}(C)$ is a valid signing of C (S73). If valid, the client will be successfully authenticated (S74, S75).

Please replace paragraph [49] beginning at page 12, with the following rewritten paragraph:

[49] Such a process is illustrated in Fig. 8. The first time the client requests an authentication from a particular server, the client sends a request to the server (S80) and the server generates a challenge C (S81), which is sent to the client (S82). The client signs C (S83) and sends $S_{PRIVK}(C)$ to the server. The server verifies (S84) the signed challenge and if the signing is verified (S85), the client is informed of success and is authenticated. If not, the client is informed of failure. The server includes a challenge C' with its response. The next time that client seeks to authenticate itself with that server, the client uses C' as the challenge, in a one round-trip authentication.